RGPD

Reglamento General de Protección de Datos

Contenido

1. INTRODUCCIÓN 2
2. NOVEDADES SIGNIFICATIVAS 2
3. DERECHOS DE LOS INTERESADOS 2
   3.1 LOPD 2
   3.2 RGPD 3
4. RELACIONES RESPONSABLE Y ENCARGADO 4
5. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO 4
   5.1 Protección de datos desde el diseño 4
   5.2 Protección de datos por defecto 5
6. RESPONSABILIDAD PROACTIVA 5
7. DELEGADO DE PROTECCIÓN DE DATOS (DPD) 9
8. PROYECTO LOPD - NOVEDADES 10
9. REGLAMENTO DE PRIVACIDAD ELECTRÓNICA 10
10. RÉGIMEN SANCIONADOR 11

1. INTRODUCCIÓN

Momentos clave:

1) ***Reglamento (UE) 2016/679 (Reglamento general de protección de datos - RGPD)*** - entró en vigor el 24 de mayo de 2016 y será de plena aplicación el 25 de mayo de 2018.

2) ***Proyecto de Ley Orgánica de Protección de Datos*** - incertidumbre en relación a su aprobación y entrada en vigor antes del 25 de mayo de 2018.

3) ***Reglamento e-Privacy*** - Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas).

2. NOVEDADES SIGNIFICATIVAS

El RGPD incluye novedades, entre otros, en los siguientes ámbitos:

- Base de Legitimación.
- Consentimiento inequívoco.
- Deber de Información: Transparencia.
- Derechos de los interesados.
- Relaciones Responsable-Encargado de Tratamiento.
- Protección de datos desde el diseño y por defecto.
- Principio de Responsabilidad Proactiva: Medidas.
- DPO: Data Protection Officer (Delegado de Protección de Datos).

3. DERECHOS DE LOS INTERESADOS

3.1 LOPD

LOPD, tiene los derechos **ARCO**:



Acceso



Rectificación



Cancelación



Oposición

DERECHO DE ACCESO – permite al ciudadano conocer y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento.

DERECHO DE RECTIFICACIÓN - se caracteriza porque permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

DERECHO DE CANCELACIÓN - permite que se supriman los datos que resulten ser inadecuados o excesivos sin perjuicio del deber de bloqueo recogido en la LOPD.

DERECHO DE OPOSICIÓN - es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo.

3.2 RGPD

RGPD, incluye nuevos derechos:



DERECHO DE SUPRESIÓN - permite que se supriman los datos que resulten ser inadecuados o excesivos. Es el antiguo derecho de cancelación.

DERECHO AL OLVIDO - es una consecuencia de la aplicación del derecho a la supresión o borrado.

DERECHO DE PORTABILIDAD - facilitar la información al interesado en un formato de uso común y lectura mecánica.

DERECHO DE LIMITACIÓN - permite limitar los tratamientos que se estén realizando de los datos.

4. RELACIONES RESPONSABLE Y ENCARGADO

LOPD	RGPD
Sólo recoge las obligaciones del Responsable	Incluye obligaciones propias del Encargado:
El Responsable ha de ser "diligente" en la selección	Mantener un registro de actividades de tratamiento, cuando proceda.
Firma de un acuerdo de tratamiento de datos entre las partes	Determinar las medidas de seguridad aplicables
Obligaciones adicionales	Designar un DPD cuando proceda
	El Responsable ha de ofrecer garantías en su elección de encargados o sub-encargados
	El acuerdo entre las partes amplía su contenido de forma significativa

Responsables y encargados podrán adherirse a códigos de conducta o certificarse dentro de los esquemas de certificación previstos en el RGPD.

5. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

PROTECCIÓN DE DATOS DESDE EL DISEÑO - El Responsable, antes de iniciar el tratamiento y cuando éste se esté desarrollando, deberá adoptar medidas que garanticen la aplicación efectiva del RGPD.

PROTECCIÓN DE DATOS POR DEFECTO - El Responsable deberá adoptar medidas que garanticen que por defecto SÓLO se traten los datos personales que sean NECESARIOS para los fines específicos del tratamiento.

5.1 Protección de datos desde el diseño

PROACTIVO, NO REACTIVO. Preventivo, no Correctivo. Anticipar y prevenir situaciones de invasión de la privacidad.

PRIVACIDAD COMO COMPONENTE ESENCIAL EN EL DISEÑO DE SOLUCIONES. Configuración predeterminada. Las tecnologías deben de estar configuradas desde inicio para proteger la privacidad.

NO SACRIFICAR PRIVACIDAD POR FUNCIONALIDAD, ni al revés.

CICLO DE VIDA DEL DATO COMPLETO. Garantizar una administración segura desde su obtención hasta su destrucción, pasando por todas las fases de su tratamiento.

TRANSPARENCIA. El sistema de tratamiento es conocido por las partes afectadas, las expectativas de privacidad se cumplen, y pueden ser verificadas por terceros.

RESPETO DE LA PRIVACIDAD DE LOS USUARIOS. Los intereses de las personas afectadas por los tratamientos se tienen en cuenta en la adopción de decisiones y medidas.

5.2 Protección de datos por defecto

Por defecto, solo serán objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

La obligación se extiende a:

- La cantidad de datos recogidos.
- La extensión de su tratamiento.
- El plazo de conservación.
- La accesibilidad.

Los datos personales solo deben conservarse durante el tiempo que se precisen como manifestación del principio de minimización de datos.

Será necesario garantizar que los datos personales no sean accesibles a un número indeterminado de personas.

Aplicar la configuración de privacidad más estricta con carácter automático cuando un cliente adquiere un nuevo producto o servicio.

Redes sociales. El usuario podrá modificar posteriormente de manera manual las opciones de privacidad de su cuenta/perfil.

6. RESPONSABILIDAD PROACTIVA

Capítulo IV, Sección 2 del RGPD **- Seguridad de los datos personales** (art. 32 y siguientes)

Aplicar medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al **riesgo**:

- Garantizar confidencialidad, integridad, disponibilidad y resiliencia.
- Capacidad de restaurar disponibilidad y acceso a los datos.
- Procesos de verificación, evaluación y valoración de la eficacia de las medidas adoptadas.
- Evaluar la adecuación del nivel de seguridad teniendo en cuenta los riesgos (Análisis de riesgos).

SEUDONIMIZACIÓN | CIFRADO DE DATOS | ANÁLISIS DE RIEGOS | EVALUACIÓN DEL IMPACTO | BRECHAS DE SEGURIDAD

Seudonimización

SEUDONIMIZACIÓN - sustituir un dato por otro.

- Seguirá existiendo la posibilidad de vincular la información a la persona física pero de manera *indirecta*.

  Ejemplo: sustituir el nombre por un código.

- Importante: Custodia *segura* de la información que permite vincular el dato seudonimizado con el titular.

- Control del Riesgo: es una medida para *mitigar* el riesgo.



Cifrado de datos

CIFRADO DE DATOS – codificar los datos para que dejen de estar en su formato original y no se puedan leer.

- Considearación 83 del RGPD: evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el *cifrado*.
- Protege la información contra amenazas (por ej. malware) y el acceso no autorizado.
- Seguridad en la transmisión e intercambio de datos.

Informe 0494/2009 AEPD

«Los productos que generan archivos PDF o el realizado por WinZip tienen *vulnerabilidades conocidas* y se disponen de herramientas de libre distribución que aprovechan dichas vulnerabilidades. Más concretamente, no sólo se pueden obtener en Internet fácilmente utilidades que rompen las protecciones de los archivos PDF o ZIP, sino que el propio algoritmo en el que descansa la cifra de documentos PDF, el algoritmo RC4, es manifiestamente *vulnerable*.»

Análisis de riesgos

ANÁLISIS DE RIESGOS - evaluar si en un tratamiento de datos existe un alto riesgo para los derechos y libertades de los interesados.



Evaluación del impacto

EVALUACIÓN DEL IMPACTO - se realizará antes de iniciar el tratamiento en caso de probabilidad alta de riesgo para derechos y libertades de los interesados.

El RGPD determina que hay alto riesgo:

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos o que afecten a los interesados significativamente.
- Tratamiento a gran escala de datos sensibles.
- Observación sistemática a gran escala de una zona de acceso público.

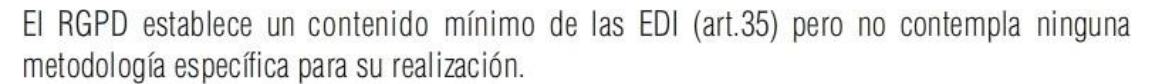


G29 ➡ para valorar si el tratamiento se realiza a gran escala debe tenerse en cuenta:

- El número de interesados afectados o en términos absolutos o como proporción de una determinada población.
- El volumen de datos y la variedad de éstos.
- La duración o permanencia de la actividad de tratamiento.
- La extensión geográfica de la actividad de tratamiento.

Las Autoridades de Protección de Datos confeccionarán listas adicionales de tratamientos que Sistemas de Información requieran una *EDI* (Evaluación del impacto).

También podrán confeccionar listados con tratamientos que NO requieran *EDI* (Evaluación del impacto).



El RGPD establece un contenido mínimo de las EDI (art.35) pero no contempla ninguna metodología específica para su realización.

- Guía de evaluación de impacto en la protección de datos del G29 (4/04/17)
- Guía sobre la evaluación de impacto relativa a la protección de datos RGPD de la Autoridad Catalana de Protección de Datos (junio 2017)

Brechas de seguridad

BRECHAS DE SEGURIDAD - No es una obligación nueva, ya se preveía en el sector de los prestadores de servicios de comunicaciones electrónicas.

- Responsable: notificación de violaciones de seguridad a la *Autoridad de Control* y al *interesado*.
- Encargado de tratamiento: notificar al responsable las violaciones de seguridad de las que tenga conocimiento.

NO será necesario hacer la comunicación si es improbable que la violación de seguridad constituya un riesgo para los derechos y libertades de los interesados.



COMUNICACIÓN A LA AUTORIDAD DE CONTROL

- Sin dilación indebida.
- Máximo 72 hrs. desde su conocimiento. Si se sobrepasa, indicar motivos de dilación.
- Contenido de la comunicación (art. 33.3): naturaleza de la violación, categorías y número de afectados y registros. Datos del DPD (si existe), consecuencias de la violación, medidas adoptadas o propuestas para poner remedio.
- Si no es posible facilitar la información en su totalidad se podrá facilitar de manera gradual pero sin dilación indebida.
- Documentar todos los hechos.



COMUNICACIÓN AL INTERESADO

- Sin dilación indebida.
- *Lenguaje claro y sencillo.*
- Contenido de la comunicación: naturaleza de la violación, datos del DPD (si existe), consecuencias de la violación, medidas adoptadas o propuestas para poner remedio.



NO será necesario hacer la comunicación:

- Si se han adoptado medidas de protección apropiadas y se han aplicado a los datos afectados por la violación.
- Se han tomado medidas ulteriores que garanticen que ya no existe probabilidad de que se concretice el alto riesgo para derechos y libertades.
- Suponga un esfuerzo desproporcionado. Opción: comunicación pública o medida semejante

7. DELEGADO DE PROTECCIÓN DE DATOS (DPD)

Es obligatorio nombrar un **DELEGADO DE PROTECCIÓN DE DATOS (DPD):**

- En autoridades y organismos públicos.
- Cuando se realicen tratamientos que requieran observación habitual y sistemática de interesados a gran escala.
- Tratamiento a gran escala de datos sensibles.

Su nombramiento y datos de contacto se harán públicos y se comunicarán a las autoridades de supervisión pudiendo tratarse tanto de personas físicas como jurídicas externas a la organización.

El **DPD** deberá disponer de cualificación profesional y contar con conocimientos jurídicos y técnicos aplicados al tratamiento de datos. Asimismo, deberá disponer de total autonomía y reportará al nivel superior de la organización.

8. PROYECTO LOPD - NOVEDADES

- Se regula el acceso a los datos de personas fallecidas por parte de sus herederos.
- Incluidos los datos de contacto y de empresarios individuales.
- Se adopta el principio de "Transparencia".
- Se regulan los sistemas de información crediticia.
- Se regula la videovigilancia.
- Sistemas de exclusión publicitaria.
- Sistemas de denuncias internas del sector privado: licitud de las denuncias anónimas.

9. REGLAMENTO DE PRIVACIDAD ELECTRÓNICA

Reglamento de privacidad electrónica - Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas (Reglamento e-privacy).

- Pretende garantizar la coherencia con el RGPD. Lo completa respecto a los datos de comunicaciones electrónicas que se consideren personales.
- Incrementar el nivel y eficacia de protección de la vida privada y datos personales tratados en las comunicaciones electrónicas.
- Derogará la directiva de la que trae causa la LSSI.
- De aplicación directa en todos los Estados miembros.
- Entrará en vigor de manera simultánea con el RGPD.
- Regulará todas las tecnologías que tratan datos, tanto si son personales como si no lo son:

  → Direcciones MAC, IMEI, direcciones IP, web bugs, pixels….

- Contiene disposiciones encaminadas a garantizar la confidencialidad de las comunicaciones electrónicas.
- Disposiciones para proteger la información emitida por equipos terminales, que pueden permitir identificar a usuarios finales.
- Comunicaciones de máquina a máquina (**Internet de las cosas**): trasporte de señales a través de una red.
- Se aplica a datos de comunicaciones electrónicas que utilicen servicios de comunicaciones electrónicas y redes públicas de comunicaciones.
- Las comunicaciones electrónicas son confidenciales: prohibido interferir en su transmisión y durante su transporte hasta la recepción por el destinatario

10. RÉGIMEN SANCIONADOR

- Para ambas normas se aplica el mismo régimen sancionador: el del RGPD.
    - **Reglamento e-privacy** Infracción del principio de confidencialidad de las comunicaciones: multa administrativa de máximo 20 millones de € o 4% máximo del volumen de negocios anual total.
    - **RGPD** Infracción de obligaciones de responsable y encargado (seguridad de los datos personales): multa administrativa de máximo 10 millones de € o 2% máximo del volumen de negocios anual total.
- Para determinar la cuantía de la sanción, la autoridad de control tendrá en cuenta circunstancias "atenuantes" o "agravantes": intencionalidad, negligencia, infracciones anteriores, medidas tomadas para paliar daños y perjuicios, etc.